DETAILED ACTION

Claims 1-5,7-32 are pending.

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with William Schaal on 11/19/2009.

The application has been amended as follows:

1. (Currently Amended) A descrambler comprising:

a non-volatile memory to store a unique key;

a control word key ladder logic to produce (i) a first value generated based on a seed ~~conditional access (CA) random~~ value and the unique key, (ii) a second value generated using the first value, the second value being a mating key recovered by performing a decryption operation on a mating key generator using the first value, the mating key generator being a message comprising one or more of the following: a manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number, and (iii) a third value recovered by a cryptographic operation using the second value;

a first cryptographic unit to descramble incoming content in a scrambled format based on the third value; and

a second cryptographic unit to decrypt incoming encrypted data using the first value.

2. (Original) The descrambler of claim 1 being a single integrated circuit.

3. (Original) The descrambler of claim 1 implemented within a set-top box.

4. (Currently Amended) The descrambler of claim 1, wherein the first value is a derivative key generated by performing a decryption operation on the seed ~~CA random~~ value using the unique key.

5. (Currently Amended) The descrambler of claim 1, wherein the first value is a derivative key derived by performing a decryption operation on a combination of the seed ~~CA random~~ value and padding data~~, the combination being at least 128-bits in length~~.

6. (Canceled).

7. (Original) The descrambler of claim 5, wherein the second value is a mating key recovered by performing a decryption operation on at least 128-bits of data comprising a mating key generator being a message comprising one or more of the following: a manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number.

8. (Currently Amended) The descrambler of claim 1[[6]], wherein the third value is a control word recovered by performing a decryption operation on an encrypted control word using the mating key.

9. (Original) The descrambler of claim 7, wherein the third value is a control word recovered by performing (i) a first decryption operation using the mating key on a first combination of a first encrypted control word and a second encrypted control word, and (ii) a second decryption operation using the mating key on a second combination of a third encrypted control word and a plurality of bits operating as padding for the second combination to be at least 128-bits in length.

10. (Original) The descrambler of claim 1 further comprising a third cryptographic unit to encrypt the descrambled incoming content prior to transmission to a digital device.

11. (Original) The descrambler of claim 10 further comprising a copy protection ladder logic to produce a copy protection key used by the third cryptographic unit to encrypt the descrambled incoming content.

12. (Currently Amended) The descrambler of claim 11, wherein the copy protection ladder logic to produce a copy protection key by performing a decryption operation on a concatenation of a seed ~~random~~ value and a plurality of bits to produce a result being at least 128-bits in length, using a logical derivation being a result of an Exclusive OR (XOR) operation of the unique key and a predetermined value.

13. (Currently Amended) A descrambler comprising:

a control word key ladder logic to produce (i) a first value generated from a cryptographic operation on a seed ~~first random~~ value using a unique key, (ii) a second value recovered from a mating key generator undergoing a cryptographic operation using the first value where the mating key generator is a message that comprises at least one of a set-top-box manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number, and (iii) a control word recovered by decrypting an encrypted control word using the second value; and

a first cryptographic unit to descramble incoming content in a scrambled format using the control word.

14. (Original) The descrambler of claim 13 being a single integrated circuit.

15. (Original) The descrambler of claim 13 further comprising a second cryptographic unit to decrypt incoming encrypted program data received out-of-band by a digital device implemented with the descrambler.

16. (Original) The descrambler of claim 15, wherein the encrypted program data comprises an encrypted entitlement management message that comprises at least two of (i) a smart card identifier, (ii) a length field, (iii) a mating key generator, (iv) at least one key identifier and (v) at least one key associated with the at least one key identifiers.

17. (Currently Amended) The descrambler of claim 16, where the mating key generator is part of the encrypted entitlement management message ~~being a message comprising one or more of the following: a manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number~~.

18. (Currently Amended) The descrambler of claim 13 further comprising a copy protection ladder logic to produce a copy protection key based on a plurality of process blocks, wherein

a first process block configured to generate a derivative key based on a second seed ~~random~~ value and either the unique key or a logical derivation of the unique key,

a second process block configured to recover a user key from an encrypted user key using the derivative key, and

a third process block configured to generate a copy protection key from a copy protection key generator using the user key.

19. (Original) The descrambler of claim 18 further comprising a third cryptographic unit to encrypt the descrambled incoming content using the copy protection key prior to transmission to a digital device.

20. (Original) The descrambler of claim 18 further comprising a one-time programmable, non-volatile memory coupled to the control word key ladder logic and the copy protection ladder logic, the non-volatile memory to store the unique key.

21. (Original) The descrambler of claim 19 further comprising a memory to store the copy protection key, the memory being coupled to the third cryptographic unit.

22. (Previously Presented) A descrambler comprising:

a memory to store a unique key;

a control word key ladder logic coupled to the memory, the control word ladder logic comprising

a first process block configured to generate a first derivative key of the unique key,

a second process block configured to generate a mating key from a mating key generator using the first derivative key, the mating key generator being a message that comprises at least one of a set-top-box manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number, and

a third process block configured to recover a control word by decrypting an encrypted control word using the mating key; and

a first cryptographic unit coupled to the control word key ladder logic, the first cryptographic unit to descramble incoming content in a scrambled format using the control word.

23. (Original) The descrambler of claim 22 being a single integrated circuit.

24. (Original) The descrambler of claim 22 further comprising a second cryptographic unit to decrypt incoming encrypted program data received out-of-band by a digital device implemented with the descrambler.

25. (Original) The descrambler of claim 24, wherein the encrypted program data comprises an encrypted entitlement management message that comprises at least two of (i) a smart card identifier, (ii) a length field, (iii) a mating key generator, (iv) at least one key identifier and (v) at least one key associated with the at least one key identifier.

26. (Original) The descrambler of claim 22 further comprising a copy protection ladder logic coupled to the first cryptographic unit, the copy protection ladder logic comprising

a fourth process block configured to generate a second derivative key based on a random value and the unique key;

a fifth process block configured to decrypt an encrypted user key using the second derivative key to recover a user key; and

a sixth process block configured to generate a copy protection key from a copy protection key generator using the user key.

27. (Original) The descrambler of claim 26 further comprising a second cryptographic unit to encrypt the descrambled incoming content using the copy protection key prior to transmission to a digital device.

28. (Currently Amended) A descrambler comprising:

a non-volatile memory to store a plurality of unique keys;

a control word key ladder logic to produce (i) a plurality of derivative keys generated based on a seed ~~conditional access (CA) random~~ value and a corresponding plurality of unique keys, (ii) a plurality of mating keys generated using the plurality of derivative keys, wherein the plurality of mating keys comprise at least a first mating key generated by performing at least one transformation on a mating key generator using the plurality of unique keys, the mating key generator being a message that comprises at least one of a manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number, and (iii) a plurality of control words recovered using the plurality of mating keys; and

a first cryptographic unit to descramble incoming content in a scrambled format based on at least one of the plurality of control words.

29. (Currently Amended) The descrambler of claim 28, wherein the plurality of derivative keys comprising:

(i) a first derivative key generated by the seed ~~CA random~~ value undergoing at least three transformations in succession, wherein a first transformation is performed on the seed ~~CA random value~~ using a first unique key of the plurality of unique keys to produce a first result, a second transformation is performed on the first result using a second unique key of the plurality of unique keys to produce a second result, and a third transformation is performed on the second result using a third unique key of the plurality of unique keys to produce the first derivative key,

(ii) a second derivative key is generated by the seed ~~CA random~~ value and a first predetermined value undergoing a bitwise logical operation to produce a fourth result, followed by the fourth result undergoing at least three transformations in succession, wherein a fourth transformation is performed on the fourth result using the first unique key to produce a fifth result, a fifth transformation is performed on the fifth result using the second unique key to produce a sixth result, and a sixth transformation is performed on the sixth result using the third unique key to produce the second derivative key, and

(iii) a third derivative key is generated by the seed ~~CA random~~ value and a second predetermined value, differing from the first predetermined value, undergoing a bitwise logical operation to produce a seventh result, followed by the seventh result undergoing at least three transformations in succession, wherein a seventh transformation is performed on the seventh result using the first unique key to produce an eighth result, a eighth transformation is performed on the eighth result using the second unique key to produce a ninth result, and a ninth transformation is performed on the ninth result using the third unique key to produce the third derivative key.

30. (Currently Amended) The descrambler of claim 28, wherein the plurality of mating keys comprising

(i) [[a]] the first mating key generated by [[a]] the mating key generator~~, being a message that comprises at least one of a manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number,~~ undergoing at least three transformations in succession, wherein a first transformation being performed on the mating key generator using a first derivative key of the plurality of derivative keys to produce a first result, a second transformation being performed on the first result using a second derivative key of the plurality of derivative keys to produce a second result, and a third transformation being performed on the second result using a third derivative key of the plurality of derivative keys to produce the first mating key,

(ii) a second mating key generated by the mating key generator and a first predetermined value undergoing a bitwise logical operation to produce a third result, followed by the third result undergoing at least three transformations in succession, wherein a fourth transformation being performed on the third result using the first derivative key to produce a fourth result, a fifth transformation being performed on the fourth result using the second derivative key to produce a fifth result, and a sixth transformation being performed on the fifth result using the third derivative key to produce the second mating key, and

(iii) a third mating key is generated by the mating key generator and a second predetermined value, differing from the first predetermined value, undergoing a bitwise logical operation to produce a sixth result, followed by the sixth result undergoing at least three transformations in succession, wherein a seventh transformation being performed on the sixth result using the first derivative key to produce an seventh result, a eighth transformation being performed on the seventh result using the second derivative key to produce an eighth result, and a ninth transformation being performed on the eighth result using the third derivative key to produce the third mating key.

31. (Original) The descrambler of claim 28, wherein the plurality of control words comprising

(i) a first control word recovered by a first encrypted control word undergoing at least three transformations in succession, wherein a first transformation being performed on a first encrypted control word using the first mating key of the plurality of mating keys to produce a

first result, a second transformation being performed on the first result using a second mating key of the plurality of mating keys to produce a second result, and a third transformation being performed on the second result using a third mating key of the plurality of mating keys to produce the first control word,

(ii) a second control word recovered from a second encrypted control word and a first predetermined value undergoing a bitwise logical operation to produce a third result, followed by the third result undergoing at least three transformations in succession, wherein a fourth transformation being performed on the third result using the first mating key to produce a fourth result, a fifth transformation being performed on the fourth result using the second mating key to produce a fifth result, and a sixth transformation being performed on the fifth result using the third mating key to produce the second control word, and

(iii) a third control word recovered from a third encrypted control word and a second predetermined value, differing from the first predetermined value, undergoing a bitwise logical operation to produce a sixth result, followed by the sixth result undergoing at least three transformations in succession, wherein a seventh transformation being performed on the sixth result using the first mating key to produce an seventh result, a eighth transformation being performed on the seventh result using the second mating key to produce an eighth result, and a ninth transformation being performed on the eighth result using the third mating key to produce the third control word.

32. (Original) The descrambler of claim 30, wherein the bitwise logical operation is an Exclusive OR operation.

Allowable Subject Matter

Claims 1-5 and 7-32 are allowed.

The following is an examiner's statement of reasons for allowance: The prior art fails to teach "the second value is a mating key recovered by performing a decryption operation on a mating key generator using the first value, the mating key generator being a message comprising one or more of the following: a manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number". The prior art further fails to teach "the plurality of mating keys comprise at least a first mating key generated by performing at least one transformation on a mating key generator using the plurality of unique keys, the mating key generator being a message that comprises at least one of a manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number." The specification further describes "the descrambler" as a single integrated circuit (abstract, [0062]). The descrambler is further described as containing "no firmware and no software" ([0070]).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RANDAL D. MORAN whose telephone number is (571)270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Randal D. Moran/
Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435